Password length: This term is used herein to refer to the number of alpha, numeric and special characters in a password guess or in a targeted password.

Pattern: This term is used herein to refer to any statistical, mathematical or otherwise related arrangement of alpha, numeric and special characters within a plurality of words or keys that may be found in an input dictionary.

Physical sequence shape: This term is used herein to refer to a memorable shape or profile formed by a set of contiguous characters in a keyboard pattern.

Primary dictionary: This term is used herein to refer to a larger attack dictionary principally used to generate password guesses.

Probabilistic password cracking system: This term is used herein to refer to a methodology and model of effectively and efficiently making password guesses of a targeted password through the use of probability values assigned to the password guesses or to structures associated with the password guesses.

Probability smoothing: This term is used herein to refer to the technique of assigning probabilities to values not found in the training set (i.e., the plurality of dictionaries, other keys or words used or known password strings). For example, a variant of Laplacian smoothing may be used to assign probabilities to all digit strings, special strings, alpha strings, and base structures.

Probability value: This term is used herein to refer to the numerical quantity of the relative likelihood of a password guess or other related structure correctly matching the targeted password.

Relevant pattern: This term is used herein to refer to a memorable configuration of characters used in a password string, where the configuration may be a single word, multi-words, repetitive words, or random, etc.

Repetitive alpha string: This term is used herein to refer to a sequence or combination of alphabetic characters that repeats in the M-word algorithm.

R-pattern: This term is used herein to refer to a relevant pattern containing a repeated string of non-words or patterns, such as the string "xyzxyz".

R-word: This term is used herein to refer to a relevant pattern containing one or more repeated words, such as the string "boatboat".

Secondary dictionary: This term is used herein to refer to a smaller attack dictionary used for additional utility (i.e., in addition to the primary dictionary) on the success of the password cracking.

Special character: This term is used herein to refer to any sequence or combination of non-alpha and non-digit symbols. For example, non-alpha and non-digit symbols may include !@#$%ˆ&*( )- . . . =+[ ]{ };':",./< >?.

Special symbol structure: This term is used herein to refer to a pure keyboard component that contains special symbols only for consideration in assigning probability values.

Substructure: This term is used herein to refer to a particular component or substring of a base structure, such as, for example, the alpha component, the digit component, and/or the special character component.

Targeted group: This term is used herein to refer to a population of people or number of targeted passwords that have relation to each other or form a pattern. For example, a "targeted group" based on language may derive word-mangling rules of suffixes based on that language, or a "targeted group" based on password creation policies may derive word-mangling rules that contain at least one numeric character, at least one special character, and at least one uppercase alpha character.

Targeted password: This term is used herein to refer to a sequence or combination of alpha, numeric and/or special characters that is subject to password guesses made by an operator of the novel probabilistic password cracking system.

Word-mangling rules: This term is used herein to refer to a set of regulations or guidelines for a password cracking system to utilize when making password guesses off of a key or word found in an input dictionary. "Word-mangling rules" can be manually preset or can be automatically generated based on patterns in the input dictionaries or in the targeted group. Examples of word-mangling rules include, but are not limited to, adding numbers to the end of words, reversing words, duplicating words, uppercasing words, inserting other characters within words, among an endless multitude of possible rules.

The advantages set forth above, and those made apparent from the foregoing description, are efficiently attained. Since certain changes may be made in the above construction without departing from the scope of the invention, it is intended that all matters contained in the foregoing description or shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.

It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described, and all statements of the scope of the invention that, as a matter of language, might be said to fall therebetween.

What is claimed is:

1. One or more tangible non-transitory computer-readable media having computer-executable instructions for performing a method of running a software program on a computing device, the computing device operating under an operating system, the method including issuing instructions from the software program for a computer processor to generate a probabilistic password cracking system for cracking a targeted password for a secured user account associated with a user, the instructions comprising:

receiving a plurality of known password strings, said plurality of known password strings formed of at least one category selected from the group consisting of alpha strings, digits, and special characters;

deriving one or more base structures from said plurality of known password strings, whereby one base structure may include more than one password string from said plurality of known password strings;

automatically incorporating a keyboard pattern into said one or more base structures, said keyboard pattern contained within at least one password string of said plurality of known password strings, said keyboard pattern being a sequence of contiguous characters starting from a particular key without regards to actual characters typed but uses a physical sequence shape of the actual characters;

automatically assigning a set of probability values to each base structure of said one or more base structures based on a probability value of each alpha string, each digit, each special character, or each keyboard pattern in said each base structure;

creating a probabilistic context free grammar based on said set of probability values assigned to said each base structure;

receiving one or more input dictionaries containing a plurality of sequences of alpha characters;